

# SecureIIS™ Web Server Protection

## Proactive Web Server Security

**V**ulnerabilities in software applications are responsible for the majority of network security breaches. Specifically, web server applications like Microsoft's IIS are consistently the most targeted for attack. Because web servers often provide a portal to your internal network, they require a more formidable and customized level of protection above and beyond what network firewalls or intrusion detection systems can provide.

Developed by eEye® Digital Security as the first-ever IIS application firewall, SecureIIS™ operates within IIS to actively inspect all incoming requests at each stage of data processing. In this way, SecureIIS prevents potentially damaging network traffic — whether encrypted or unencrypted — from penetrating your servers.

### True Application Layer Protection

eEye Digital Security introduced the concept of application-layer protection, which has revolutionized proactive security. Unlike network-layer protection products, an application-layer solution works within the application that it is protecting. SecureIIS inspects requests as they come in from the network level, as they are handed off at the kernel level, and at every level of processing in between. If at any point SecureIIS detects a possible attack, it can take over and prevent unauthorized access and/or damage to the web server.

### Integrated into the IIS Platform

SecureIIS was developed as an ISAPI filter, which allows it to integrate more tightly with the web server. SecureIIS monitors data as it is processed by IIS and can block a request at any point if it resembles one of many classes of attack patterns. Because of eEye's extensive knowledge of the various ways in which IIS servers can be attacked, as well as the nature of an application firewall, even undiscovered vulnerabilities specific to IIS are secured.

### Blocks Against Entire Classes of Known & Unknown Attacks

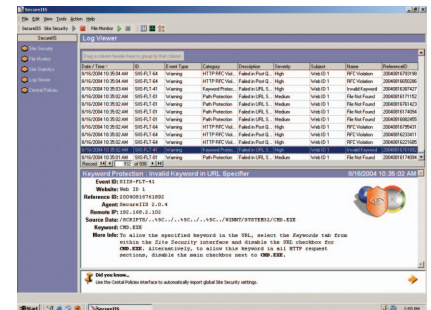
Unlike network firewalls and intrusion detection systems, SecureIIS does not rely upon a database of attack signatures that require regular updating. Instead, it uses multiple security filters to inspect web server traffic for such issues as buffer overflows, parser evasions, directory traversal and other attacks. Therefore, SecureIIS is able to block entire classes of attacks, including those attacks that have not yet been discovered.

### Created by the Experts on IIS Vulnerability

Worldwide, eEye is recognized as one of the most trusted and respected sources dedicated to improving IIS security. In fact, eEye's research team is credited with the discovery of numerous high-severity IIS vulnerabilities that would have allowed an attacker to gain complete remote control over a susceptible server.

### Fast Facts

- Runs on Windows NT 4 (IIS 4), Windows 2000 (IIS 5), or Windows 2003 (IIS6)
- Integrated technology does not affect server performance
- Compatible with and protects all common web-based applications such as Flash, Cold Fusion, FrontPage, Outlook Web Access and more
- Protects against the following classes of attacks: buffer overflow, parser evasion, directory traversal, general exploitation, high-bit shellcode protection, and more



eEye Digital Security®

# SecurellS™ Web Server Protection

## Additional Features and Benefits

- **Central Policy Management**  
SecurellS provides the ability to manage settings for any number of machines from a single, central location.
- **Award Winning Graphical User Interface**  
SecurellS configuration options are managed through an easy-to-use interface. Logs and real-time statistical charts are easily navigated.
- **Logging of all Blocked Requests**  
The SecurellS log provides detailed explanations as to why requests were denied.
- **Run-Time Switching**  
Configurations can be modified without having to restart the web server, thus preventing disruption of the active website.
- **Real-Time Statistic Charts**  
Monitors activity in real-time by providing graphs based on class of attack.
- **Non-Intrusive Protection**  
SecurellS offers protection without affecting service levels on your web server. In fact, SecurellS can even provide improved performance when the web server is under attack.
- **Third-Party Application Protection**  
SecurellS stops attacks launched against third-party web server applications or custom web scripts.
- **Protection Over SSL Encrypted Sessions**  
SecurellS stops attacks on encrypted sessions based on the ability to analyze the content of HTTPS sessions before and after SSL encryption.
- **Flexible Export Capability**  
The SecurellS log can be exported in any number of different formats including tab delimited, text, Excel, SQL and more.
- **Compatible with Web-Based Applications**  
SecurellS works with and protects all common web-based applications such as Flash, Cold Fusion, FrontPage, and Outlook Web Access.
- **File System Activity Monitoring**  
SecurellS can send alerts when such activities as file additions, deletions and modifications occur.
- **Global-Settings Adjustment**  
SecurellS settings can be configured globally across all sites on a server, on a per site basis or on a per virtual directory basis through an intuitive point-and-click interface.

### SecurellS protects against the following attack types:

- **Buffer Overflow Attacks**  
SecurellS checks the lengths of all client-supplied buffers. If the data is larger than the maximum size allowed, SecurellS will drop the connection, thereby avoiding a buffer overflow.
- **Parser Evasion Attacks**  
Insecure string parsing can allow attackers to remotely execute commands on the machine running the web server. SecurellS checks for various characters in a string that would allow an attacker to add on commands to a normal value. If these characters are found, SecurellS will drop the connection.
- **Directory Traversal Attacks**  
In certain situations, various characters and symbols can be used to break out of the web server's root directory and access files on the rest of the file system. SecurellS checks for these characters and also blocks access to specific directories.
- **General Exploitation**  
By checking for common attacker "payloads" such as cmd.exe in the exploiting data, SecurellS can prevent an attacker from gaining unauthorized access to your web server and its data.
- **High-Bit Shellcode Protection**  
Normal English-language web traffic does not contain high-bit characters. SecurellS will drop all requests containing high bit characters, which often signal a potential buffer overflow attack.
- **RFC Compliancy**  
SecurellS prevents attackers from manipulating the HTTP protocol in attempts to bypass security systems and exploit security holes.
- **Other Attacks**  
SecurellS has additional checks in place to identify — and drop — requests that contain recognized patterns. Limitations are also placed on the size of uniform resource locators (URL/URI), HTTP variables, request methods, request header size and other HTTP-related content.

## System Requirements

- Windows NT 4.0, IIS 4.0 and Service Pack 6; or
- Windows 2000, IIS 5.0 and Service Pack 1 or greater; or
- Windows 2003, IIS 6.0 and Service Pack 1 or greater

## About eEye Digital Security

eEye Digital Security is a leading developer of network security products that deliver unsurpassed levels of vulnerability protection before, during and after malicious attacks. Driven by the world-renowned eEye Research Team, the company has won numerous awards and recognition in the field of network security, including the recent top 10 recognition in the Red Herring Top 100 Innovators awards for 2004. A global company with offices, partners and distribution channels around the world, eEye helps protect the digital assets of major corporations, educational institutions, and government entities in over 80 countries.

eEye Digital Security  
www.eEye.com

U.S. Tel: 1.866.339.3732  
N. America: 1.949.900.4100  
Geneva: +41 22.718.7700  
London: +44 (0) 208.956.2270

N. America: sales@eeye.com  
International: sales.eu@eeye.com



eEye Digital Security®